Google Hacking







“Eu penso que ele está pronto para começar a usar o computador. Ele acabou de dizer 'Google!'”

Objetivos

- Entender o que é Google Hacking
- Conhecer os riscos que o Google traz
- Aprender como usar o Google como ferramenta auxiliar para um pentest
- Conhecer os principais comandos do Google
- Aprender como encontrar buscas pré definidas, utilizando o GHD

O que é Google Hacking?

- Google Hacking é a atividade de usar recursos de busca do site, visando atacar ou proteger melhor as informações de uma empresa.

- As informações disponíveis nos servidores web da empresa provavelmente estarão nas bases de dados do Google.

- Um servidor mal configurado pode expor diversas informações da empresa no Google. Não é difícil conseguir acesso a arquivos de base de dados de sites através do Google.

OYS
ACADEMY

Google Cache

- O Google armazena por um período versões anteriores de qualquer site que tenha algum dia sido indexado por seu robô de busca.

- Isso possibilita termos acesso a informações que tenham sido retiradas na versão mais atual do site, e que possam ser, de alguma maneira, sensíveis.

Web Imagens Vídeos Mapas Notícias Orkut Gmail mais ▾



4linux Pesquisar

Aproximadamente 36.100 resultados (0,26 segundos) Pesquisa avançada

Tudo

Mais

A Web

Páginas em português

Páginas de Brasil

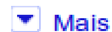
Mais ferramentas

4Linux - Linux, Software Livre, Cursos, Treinamento, Consultoria ... 

A **4Linux** oferece cursos de Linux, EaD, consultoria em software livre além de suporte e desenvolvimento com equipe 24x7 em todo Brasil.

www.**4linux**.com.br/ - Em cache - Similares





Cursos | Cursos com padrão IBM de qualidade
Fale Conosco | Metodologia de Ensino à distância ...
Empresa | Consultoria
Participe das promoções da 4Linux ... | Eventos

Mais resultados de 4linux.com.br »

OYS ACADEMY

Comandos Avançados do Google

- intitle, allintitle
- inurl, allinurl
- filetype
- allintext
- site

- link
- inanchor
- daterange
- cache
- info
- related

OYS ACADEMY

Levantamento de Informações

- O Google é a principal ferramenta para o levantamento de informações de nosso alvo.

- Por isso, vamos definir um alvo específico, e buscar toda infomação possível de conseguir através do Google sobre o mesmo. VAMOS À PRÁTICA!

- **Dica:** tente a busca "currículo + identidade + cpf", sem as aspas. Você já ouviu falar de "laranjas"? Então...

- **Google Hacking Database:**

•http://johnny.ihackstuff.com/ghdb/

•Vamos testar algumas tags do GHD e ver que tipo de informação conseguimos.

Mais prática...

- site:gov.br ext:sql
- inurl:"powered by" site:sistema.com.br
- inurl:e-mail filetype:mdb
- intitle:VNC inurl:5800 intitle:VNC
- "Active Webcam Page" inurl:8080
- intitle:"toshiba network camera - User Login"
- intitle:"Flash Operator Panel" -ext:php -wiki -cms -inurl:as
- “Microsoft-IIS/6.0” intitle:index.of

Contramedidas

- Possuir uma boa política referente à publicações de informações na internet.

- Não deixar configurações padrão em servidores web, para que os mesmos não consigam ser identificados facilmente.

- Sempre analisar as informações disponíveis sobre a empresa em sites de busca.

- Alertar e treinar os funcionários da empresa com relação a maneira com que um ataque de engenharia social pode acontecer, e as possíveis informações que o atacante poderá usar nesse ataque.



"Alguém conseguiu meu número de Segurança Social na internet e roubou minha identidade. Obrigado Deus - Odeio ser eu mesmo!"